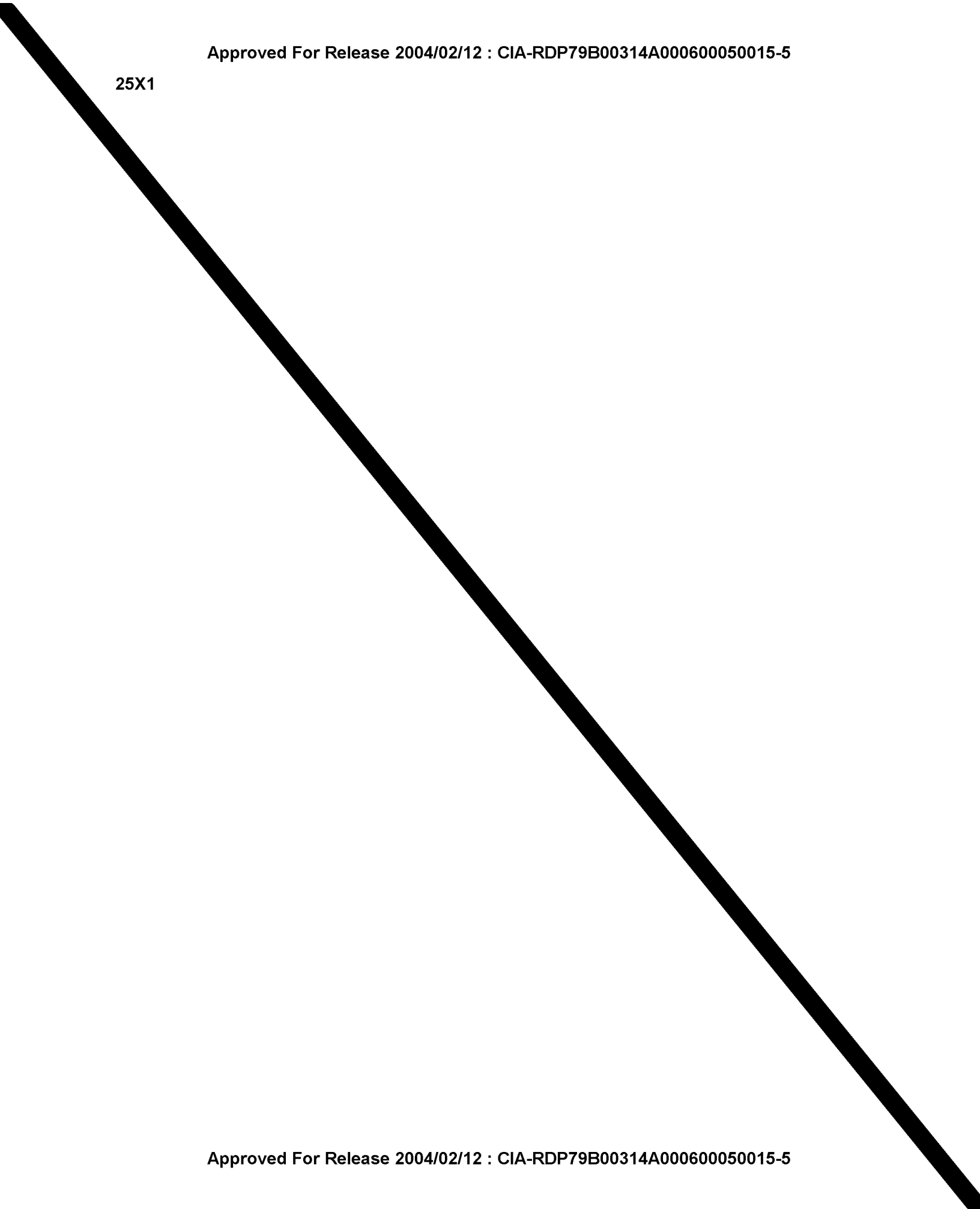
25X1



THE WEEK THE COMPUTERS STOPPED

the ultimate weapon

by HAROLD WEISS

The head of Wontonia's intelligence organization was addressing a class at his espionage school. "Comrades, you have heard of the tremendous sabotage which has recently occurred in the United States, including the complete shutdown of the leading capitalist country's economy for a significant period of time. This, as you may have guessed, was a triumph of our SUEY (Subversion Unrelenting to Entomb the Yankees) branch. We are privileged to have with us today Agent 2-5 who was in charge of this operation and who, I might add, has just been decorated with the Order of the Main Chow.

"The techniques which 2-5 will be discussing are probably applicable to most highly industrialized societies, so you have much to learn from his experience. A powerful weapon is available which a less developed country such as ours can use against the imperialists. His work has led to the computer training which you have received, so you should have no trouble with the technical aspects of his discussion. Without any more delay, I shall turn the rest of today's session over to our highly esteemed Agent 2-5."

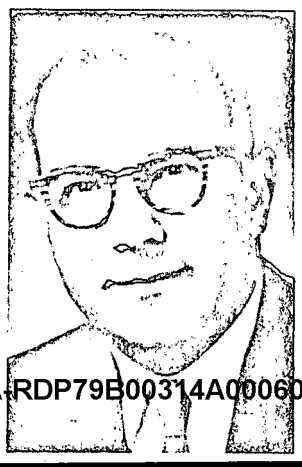
A surprisingly young, intellectual-looking man came up to the front of the room from where he had been standing in the rear. He was obviously not a Wontonian. He wasted no time in formalities.

"Comrades, there is much to cover in only a few hours, but I want to give you a little of the background on my most recent assignment. For security reasons some details will be omitted from my discussion. Several years ago the head of SUEY was given the assignment of seriously sabotaging the United States economy, performing industrial espionage, and acquiring considerable sums of United States dollars which would be useful to Wontonia in a number of ways.

"As a member of his group I had been studying this imperialist economy for some time along with other agents, searching for areas of vulnerability to sabotage. We had explored damage to such obvious essential services as electrical power, water supply, transportation, and the like, and in the process conducted some successful capers, although their over-all impact was not very significant. During this period I became aware of the growing field of information technology in the United States. Research showed the increasing vulnerability of the U.S. economy to a relatively few sophisticated machines. There was a great concentration of values at comparatively few locations. The informational life blood of all the large companies and government agencies flowed through only a thousand or so key computers. As an immature and rapidly growing field, information technology had many deficiencies that it appeared SUEY could exploit. I was given training to [illegible] this effect and was placed in charge of the project which I shall be describing to you. As you might guess, I received my current code number at the time of that promotion. My background included considerable scientific as well as business training, which is one of the reasons a project of this scope was given to a fairly young man.

"Our intelligence operations have always benefited from thorough planning and a long-range approach, I am told. This project was no exception. To be effective, not only I but the several agents initially assigned to my project had to be technically competent. There were computer manufacturers' courses available in a number of countries, university and college courses, private school training, and other sources of knowledge about information technology. Each agent received intensive training in computer programming, among other subjects. It was fairly easy to place intelligent, well-trained people in their initial jobs because of the personnel shortage in the computer field. Once they had two years or so of practical experience, their skills became highly salable and they could move from place to place readily. The computer field is characterized by considerable job-jumping, which made our task much easier. An effective agent could therefore be brought to bear against several computer installations in only a few years.

"We felt our way cautiously at first to test the lax security of computer installations and to see what we could get away with. Our people did numerous little things to reduce the efficiency of the computer operations they worked at and thereby harm the large organizations by which they were employed. We filched cards from program or data decks, put cards out of sequence, wiped out key tapes and disc packs, caused subtle equipment malfunctions, and the like. We were able to change program cards or copy magnetic tapes with changes to create program bugs



Mr. Weiss is director of the Automation Training Center, Scottsdale, Ariz., and has been active in edp since 1952. He was head of customer support for the GE computer department and is now ready to reveal his authorship of "The Konscience of a Komputer Konservative," appearing in the October, 1962, issue of Datamation. He is a CPA, a holder of the DPMA certificate and a member of the DPMA certificate testing committee.

in production programs. The [illegible] which dash things like these caused must be seen to be believed. A false fire alert at an unprepared installation usually leads to someone pressing the panic button, which can take some computers down for days.

"As we gained experience and saw how permissive things were at many computer centers, we got more ambitious. Localized fires turned out to be a very effective technique for computer sabotage. There are often extensive combustible materials present, noxious smoke often results which hampers fire fighting, and often all the major programs and files of the installation are physically close together and not in fire-resistant vaults. One such fire can knock out a highly integrated organization with most of its information system on the computer, or at least cause it to suffer catastrophic consequences. And you should see the Yankee firemen! Just turn them loose with their axes and hoses and you needn't worry about a computer center for a long time. Some places had electrical shorts for months after a fire. It was very pathetic to see the recovery attempts of some computer groups which thought they had good disaster protection. Off premises they typically kept third generation files, some obsolescent programs, inadequate transaction data, and little if any system documentation. By the time their equipment was replaced and they started to try to bring their files up to date, they were swamped with piled-up transactions—that is, where sufficient data to operate at all existed. Some companies failed completely as a result of these fires or suffered huge financial losses.

"Ours can be a grim business, but SUEY's computer project was not without its humor. One of our people heard of a planned visit by a Boy Scout troop to a large military computer installation. Typically, visitors were permitted to walk through the computer room itself during an Open House. With considerable inspiration our agent met the group at the parking lot and passed out toy magnets to the boys. Quite a few programs on magnetic tape were wiped out that day as a result of boys trying to stick their magnets on everything they could, before the problem was detected by the computer staff.

"As another example, you may be aware that many computers are placed at ground floor level or in basements. One of our enterprising agents arranged for a sewer to back up, which took out a large commercial computer installation.

"We use beautiful women in various aspects of intelligence work and their value was proved in our information technology project as well. We trained some carefully selected female agents and placed them in computer groups. Besides the direct sabotage and espionage which they performed, there were beneficial side effects from their distraction to male technical personnel. A very significant rise in program error rate could be correlated to the arrival of each such agent.

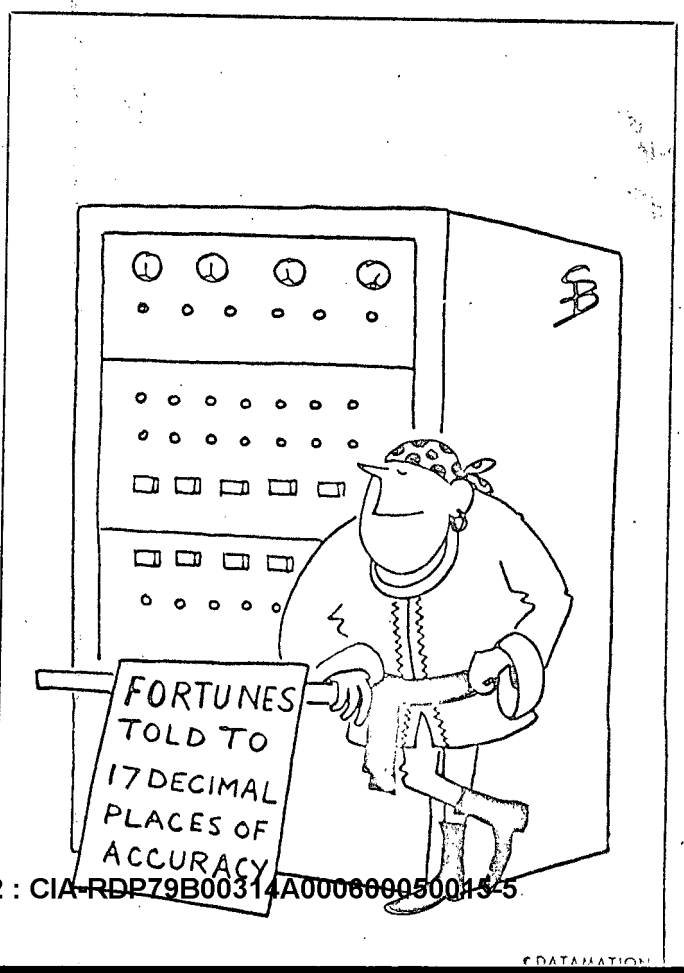
"We found that wholesale personnel raids could seriously weaken an information systems organization. Some of our people had worked up to managerial levels after a few years and could carry out such tasks directly. Others in senior positions found willing accomplices in some computer managers. I recall a data processing manager who jocularly offered the advice that one should not steal all the skilled personnel of another computer group. He recommended following conservation practices—one senior man should be left on the victim's staff to train a new set of people to be raided at a later date.

"As you can see, our plans were proving effective. I have not yet mentioned an important aspect of our assignment, which was to secure considerable sums of Yankee dollars. We found it very easy to steal proprietary materials from waste baskets in computer centers, especially during periods of debugging. Some such information could be used

[illegible] to sell. Even used carbon paper was quite valuable. There tends to be loose control of forms at U.S. computer centers, except for check forms. We were able to acquire invoice and other forms which were very useful in the perpetration of various frauds. I might mention that ample computer service bureau time is available where needed to accomplish certain frauds and at relatively nominal rates. We also stole certain programs and files and held them for ransom. You would be surprised what some computer users or their data processing insurance companies will pay for the three generations of an important master file!

"Early in our project, I personally made it a practice to walk into strange computer rooms to see how far I could go without running into trouble. Initially I did not remove materials or perform acts of sabotage; rather, it was in the nature of research. Usually after wandering around for 20 minutes or so and looking at equipment, files, and documentation as a perfect stranger, a member of the staff would walk up and ask if I needed any help. Later many of our people did perform acts of sabotage or steal materials during such unauthorized visits. I have, for example, wandered about with an Alnico magnet in my hand in a room with 10,000 tapes, tapping any at will. One day I walked out of a large oil company's computer center with a magnetic tape filled with valuable exploration data, copied it at a service bureau, and returned the original without detection. We made a good deal of money out of that particular caper. All you had to do on such raids was to be well dressed, brazen and to know a little about computers. It may seem incredible that things were so lax and permissive with these rich companies, but they were. Can you imagine billion-dollar companies that 'could-not-afford' a vault for vital magnetically stored records?

"Well, after three years we had severely damaged several



dozen large companies which had a major role in the U. S. economy and completely destroyed some smaller ones. We had also acquired almost $100,000,000 by various means. By now, however, many organizations were starting to tighten up their computer practices. Some began to treat their computer areas like a bank vault or top military security area. While it was hard to prove who performed some of the sabotage which I have described, several of our agents were being actively sought by the police, although the authorities were not yet aware of SUEY's inspiration and direction. I felt it imperative that we move more rapidly and across a broader aspect of the Yankee economy.

"Finally we recognized the Achilles heel of information technology—personnel—although I have mentioned personnel raids and other minor techniques in this category of sabotage. We had observed that many computer people were poorly motivated, had little loyalty to the organizations employing them, had no path of progress in their companies, etc. Even computer management had little participation in their companies' training and development programs. This was a prime factor in the heavy computer personnel turnover which we had exploited. After a decade or more in computer work the first blush of enthusiasm and pioneering had worn off. Much of the work was becoming more routine and less creative. There existed the specter of technological unemployment from automatic programming developments, the machines operating themselves via sophisticated programs, the machines even diagnosing their own malfunctions. Here was a really prime area for us to concentrate our efforts.

"We planned to organize information technology workers into a strong union. The ultimate weapon would be disabling strikes that could completely shut down organizations with little likelihood that strikebreakers could be brought to bear. We started very modestly, forming a few locals in the larger cities. The Computer Employees Union (CEU) was vertically organized, with operators, coders, programmers, systems people, maintenance men, even some lower level managers joining. With a few token strikes we won some large pay increases and got privileged status for computer people. As you might expect, a SUEY man headed up the national organization of CEU and we had other agents in the leadership of several strategic locals.

"Then we got a fortunate break which accelerated our entire program considerably. A large independent union saw in affiliation of the computer workers an opportunity to reinforce its own goal—the capability of shutting down the national economy to enforce a victory at the bargaining table. We got married to them in almost indecent haste. With the infusion of considerable money and powerful local support from the new parent union, organization of information technology workers proceeded rapidly.

"Finally our big moment came. The parent union called a nationwide strike. We immediately called a simultaneous walkout of the affiliated Computer Employees Union. After a week of the computers being shut down, you can hardly imagine the catastrophic impact on the U. S. economy. Most banks could no longer process checks. The credit system broke down. There were few companies which could bill customers. Plants closed because many essential functions were gone—production scheduling, purchasing, etc. The process industries shut down because our operators and maintenance people walked out. Many areas were blacked out as a result. There were no airline reservations or large magazine mailings. Many newspapers could not publish. Most of the scientific and engineering work in the country was interrupted. The military establishment was severely hurt despite the fact that some of their computer installations were manned by service personnel. You must pardon my apparent lack of modesty when I tell you that this was *total disaster*. It is essential that you grasp the full meaning of our operation.

"In desperation the federal government invoked an injunction with strong punitive features. We felt it too dangerous to our long-term plans to oppose this restraint outwardly, so the CEU people went back to work. Word was informally passed down the line, however, to sabotage computer installations wherever feasible. Operations were slowed down, people made many more errors, there was 'inadvertent' use of wrong generations of files, and so on. Programmers were always '90% done' on their assignments. Systems men messed up system designs and antagonized operating people. A rash of mysterious machine malfunctions occurred which maintenance people were slow to find. After several months of this a number of large employers caved in and CEU and our parent union won the strike. The cost to the Yankee imperialists has been conservatively estimated in the tens of billions of dollars.

"This, comrades, was only a first attempt with very limited resources, but which nevertheless produced impressive results. There is considerable opportunity for ingenuity and creative thinking by new cadres of agents such as yourselves. There is no reason why the basic pattern which I have described today can not be applied to other imperialist nations, although they may lag the Yankees by a few years in terms of their concentration of values in computer centers and thus in their vulnerability to our operations.

"This concludes my formal remarks. After a brief pause for refreshments, I shall be happy to answer any questions you may have on basic ideas or techniques, although [illegible] names, places or other details. You have been a most appreciative audience, for